Communiqué de presse, le 1er octobre 2019, Bruxelles

« Relax. Réfléchissez à deux fois avant de cliquer sur un lien »

Octobre : le mois de la cybersécurité

Dans le cadre du **Mois européen de la cybersécurité**, le Centre pour la Cybersécurité Belgique (CCB) et la Cyber Security Coalition lancent la cinquième édition de leur **campagne de sensibilisation** sur le thème de la **cybersécurité** . Cette fois encore, nous nous attaquons au phénomène du **phishing**.

Le phishing demeure le principal problème de cybersécurité qui touche les citoyens belges. Il offre aux cybercriminels une importante porte d'accès aux appareils et systèmes informatiques. Cette année (de janvier à septembre), nous avons déjà comptabilisé **plus d'un million de messages à l'adresse suspect@safeonweb.be**. L'année passée, le nombre de messages était de 648 000 pour l'ensemble de l'année. Nous assistons donc à une forte augmentation cette année.

> *« Les cybercriminels recourent au phishing pour diffuser des malware, s'approprier des données personnelles ou extorquer de l'argent. En améliorant la résilience de la population belge contre le phishing, nous faisons d'une pierre « trois » coups. Plus nous recevons de messages à l'adresse suspect@safeonweb.be, plus nous sommes en mesure de bloquer de sites. Nous bloquons les faux sites Internet d'autant plus vite lorsque les internautes nous transmettent les messages suspects dans les plus brefs délais. Plus nous agissons vite, moins il y a de victimes. Nous demandons donc à la population belge de continuer à transmettre tout message suspect à l'adresse suspect@safeonweb.be avant de l'effacer ensuite. »*
>
> - Miguel De Bruycker, directeur CCB

Tout au long du mois de la campagne, nous souhaitons attirer toute l'attention sur le thème via des spots radio, des spots publicitaires sur les médias sociaux, des bannières et autre matériel de campagne. Vous trouverez des astuces et informations utiles sur le site Internet de la campagne https://campagne.safeonweb.be/fr. Vous pourrez également vous familiariser avec l'indice santé qui vous invite à tester vos connaissances en cybersécurité. Vous pouvez télécharger tous les matériaux de la campagne sur https://safeonweb.be/fr/materiel-de-campagne

Notre message s'adresse aussi directement au citoyen : nous organisons une action dans 5 grandes gares et nous partons en tournée avec le Federal Truck dans 6 établissements universitaires.

> *« Au volant du Federal Truck, nous partons à la rencontre de la population. Nous faisons étape dans différents établissements universitaires à Bruxelles, en Wallonie et en Flandre et nous invitons les étudiants à s'intéresser de plus près au phishing »*
>
> - Phédra Clouner, directrice adjointe CCB

Des services publics fédéraux, des établissements universitaires, des petites et grandes entreprises, mais aussi des asbl et d'autres organisations soutiennent la campagne. **Cette année**, ce sont **plus de 500 partenaires** qui contribuent à la diffusion du matériel de campagne.

> *« Dans le monde des entreprises aussi, le phishing continue de poser un sérieux problème. C'est pourquoi je recommande sans hésiter aux organisations de faire usage de ce matériel gratuit afin d'armer leurs collaborateurs, leurs clients et leurs contacts professionnels contre le phishing. »*
>
> - Jan De Blauwe, président Cyber Security Coalition

L'un des partenaires qui soutiennent la campagne cette année est le site de bonnes affaires 2ememain.be. « *Nous sommes partenaires de la campagne de prévention contre le phishing* », déclare Alain Buyle, porte-parole de 2ememain.be. *« Chaque mois, des millions de personnes réalisent de bonnes affaires sur notre plateforme. Si cela se passe bien la plupart du temps, chaque cas de fraude reste néanmoins un cas de trop. En plus des mesures que nous implémentons nous-mêmes, nous aimerions relayer les conseils véhiculés par la campagne sur la façon de réaliser de bonnes affaires en toute sécurité ».*

La campagne nationale de sensibilisation contre le phishing se concentre sur les **faux messages**. De nos jours, la fraude par phishing se fait sur différentes plateformes et plus uniquement via mail : les pirates essaient de nous piéger en envoyant de faux messages via SMS, WhatsApp, Facebook Messenger et d'autres plateformes encore. Et les utilisateurs de 2ememain.be ne sont pas en reste. La forme la plus courante de piratage est celle qui conduit les internautes à transmettre leurs données confidentielles en effectuant une transaction sur une autre plateforme que celle que nous proposons sur

2ememain.be. Les pirates informatiques essaient ensuite de voler des coordonnées bancaires et d'autres données personnelles via de faux sites Internet. « *Nous conseillons à tous les utilisateurs de toujours y réfléchir à deux fois avant de cliquer sur un lien ou d'accepter de réaliser une transaction sur une autre plateforme* » explique le porte-parole de 2ememain.be Alain Buyle.

Iwein Segers et **Jérôme de Warzée** sont les coachs « santé numérique » de cette campagne.

Spots publicitaires pratiques
La campagne sera lancée le 1er octobre 2019 et se déploiera sur un mois complet. En guise d'appui, nous mettons gratuitement à disposition non seulement du matériel (posters imprimables, bannières et visuels en ligne), mais aussi des spots publicitaires pratiques. Ces spots décrivent, pas à pas, comment contrôler le niveau de sécurité d'un lien, comment reconnaître un nom de domaine suspect, comment vérifier la qualité de l'émetteur et plus encore.

Phishing, phishing et encore phishing

Identifiez les faux messages
« Au travers de cette campagne, nous voulons armer les internautes contre le phishing : les utilisateurs tant professionnels qu'occasionnels, qu'ils soient jeunes ou plus âgés », tels sont les mots de Miguel de Bruycker, directeur du Centre pour la Cybersécurité Belgique.

Les messages de phishing :

- vous parviennent la plupart du temps de manière inattendue et sans raison
- utilisent un ton directif ou essaient de susciter votre curiosité
- contiennent des fautes d'orthographe ou sont rédigés dans un style inhabituel
- se présentent à vous de manière vague ou utilisent votre adresse mail en guise de formule d'appel
- proviennent d'un émetteur inconnu
- contiennent un lien qui mène vers un site non sécurisé

« Les faux messages ne sont pas systématiquement des e-mails. De plus en plus souvent, les pirates informatiques opèrent via de faux sms. Ce phénomène a été baptisé le « Smishing ». L'on peut également recevoir des messages de phishing depuis des réseaux sociaux comme Facebook et WhatsApp. »

- Miguel De Bruycker, directeur CCB

suspect@safeonweb.be

En 2018, nous avons reçu 648 000 messages à l'adresse suspect@safeonweb.be . Cette année, nous **dépasserons la barre du million**. En 2018, nous sommes parvenus à faire bloquer 4 à 5 faux sites Internet par jour grâce à cette initiative et à l'aide de la population belge. En 2019, nous en sommes à une **moyenne de 30 faux sites Internet bloqués par jour**, soit environ **7 fois plus**.

À l'issue de cette campagne, chacun sera capable d'identifier un faux message et saura quel comportement adopter : ignorer et effacer ce message. De Bruycker : « *Mais nous allons encore plus loin. Nous demandons à chacun de transmettre tout message suspect à suspect@safeonweb.be pour ensuite l'effacer. Le CCB effectuera un scan automatique des liens et pièces jointes à l'aide d'une technologie anti-virus avancée. Les liens dangereux seront consignés dans une liste noire et bloqués par les principaux navigateurs web. C'est ainsi que nous ferons d'Internet un endroit plus sûr*. »

Les cybercriminels au sommet de la créativité

Les cybercriminels redoublent de créativité dans leurs tentatives frauduleuses :

- ils envoient des faux messages tellement convaincants que vous finissez par ouvrir l'annexe,
- ils vous promettent une importante récompense si vous complétez leur enquête et que vous divulguez vos données,
- ils vous menacent si vous ne réagissez pas,
- et ils utilisent des canaux sans cesse plus nombreux (e-mail, WhatsApp, Messenger…).

Heureusement, nombre d'internautes sont suffisamment prudents et ne tombent pas dans le panneau !

Le phishing, ça peut arriver à tout le monde

Le phishing est une technique courante pour voler des coordonnées bancaires et propager des malwares. Les cybercriminels se servent également de faux messages pour voler des données personnelles afin de prendre le contrôle de comptes en ligne, par exemple. Et cela peut arriver à tout le monde !

Cet été, le compte Instagram « Belgium. Uniquely Phenomenal » a été hacké en passant par du phishing. Les cybercriminels ont envoyé un faux e-mail qui venait soi-disant d'Instagram et qui affirmait que le compte en question comportait des problèmes de copyright. Pour y remédier, le destinataire du message devait à nouveau s'identifier par l'intermédiaire d'un lien figurant dans le message. En cliquant sur le lien, la personne

s'est retrouvée sur un faux site ressemblant comme deux gouttes d'eau à celui d'Instagram. En introduisant ses données de connexions, la personne a permis aux cybercriminels d'accéder au compte. L'information était crédible et bien écrite. L'apparence de l'e-mail n'avait rien de douteux. Bref : cela peut arriver à tout le monde. Et cela peut provoquer des catastrophes, comme des atteintes à l'image.

Heureusement, l'accès a rapidement pu être rétabli en prenant contact avec Instagram. Pour éviter d'être à nouveau victimes de phishing à l'avenir, tous les collaborateurs ont été sensibilisés et l'accès au compte Instagram a été sécurisé en mettant en place une authentification à deux facteurs (2FA).

#####

À propos du Centre pour la Cybersécurité Belgique :
Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale chargée de la coordination de la cybersécurité en Belgique. Le CCB se fixe pour objectif de superviser, de coordonner et d'assurer l'application de la stratégie belge en matière de cybersécurité. C'est grâce à un échange optimal d'informations que la population, les entreprises, les autorités et les secteurs vitaux parviendront à se protéger adéquatement.
www.ccb.belgium.be

Contact presse Centre pour la Cybersécurité Belgique

Andries Bomans
T: +32 471 66 00 06
Andries.bomans@ccb.belgium.be

Katrien Eggers
T: +32 485 76 53 36
Katrien.eggers@cert.be

À propos de la Cyber Security Coalition :
La mission de la *Cyber Security Coalition* est de renforcer la résilience de la cybersécurité en Belgique en construisant un écosystème de cybersécurité solide au niveau national. Nous le faisons en réunissant les compétences et l'expertise du monde académique, du secteur privé et des pouvoirs publics sur une plate-forme de confiance visant à favoriser l'échange d'informations, la collaboration opérationnelle, en émettant des recommandations pour des politiques et des lignes directrices plus efficaces et finalement en réalisant des campagnes de sensibilisation conjointes s'adressant aux citoyens et aux organisations.
www.cybersecuritycoalition.be

Contact presse Cyber Security Coalition
Sofie De Moerloose
T : 0478 78 96 07
info@cybersecuritycoalition.be